Notice of Allowability	Application No.	Applicant(s)	
	09/767,610	MORICONI ET AL.	
	Examiner	Art Unit	
	Brandon S Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed on November 29, 2004*.

2. ☒ The allowed claim(s) is/are *58,59,64,65,68,69,71,113-117,119,122,148 and 157-170*.

3. ☒ The drawings filed on *22 January 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Allowable Subject Matter

1. Claims 58, 59, 64, 65, 68, 69, 71, 113-117, 119, 122, 148, and 157-170 are allowed.

2. The terminal disclaimer, filed November 29, 2004, is proper.

3. The following is an examiner's statement of reasons for allowance: based on the terminal disclaimer and the arguments by applicant in the November 29, 2004, response, mainly that Nessett discloses a security policy between different nodes of a multilayer firewall system, wherein the nodes are physical devices and systems. The claimed limitations of the instant application disclose a guard located in a client to manage access to software applications at that client. It is different to access software on a particular client than it is to access a particular client, as was being taught by the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Karl Kenna, registration number 45,445, on February 2, 2005.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

IN THE CLAIMS:

58. (Amended) A system for maintaining security in a distributed computing environment comprising:

a central policy manager located at a server for managing and distributing a security policy; and

an application guard located at a client, said application guard including a customized local policy particular to that client, for managing access by a user of the client to software application components at the client, as specified by the security policy.

77-111. (Canceled).

122. (Amended) A method for maintaining security in a distributed computing environment comprising:

managing a central security policy located at a server via a policy manager; and

managing access by a user of the client via an application guard at a client to a transaction related with a software application component on that client, as specified by the security policy.

128-132. (Canceled).

136-146. (Canceled).

148. (Amended) A method of granting client access authorization comprising:

using an application guard located at a client that includes at least

requesting access to a software securable component associated with an application protected by the application guard, wherein the application guard constructs and issues an authorization request, and

evaluating the authorization request via the application guard according to its local client policy to determine whether to allow or deny the authorization request; and

wherein evaluating the authorization request includes and evaluator searching deny rules in the local client policy, and if the evaluator finds a deny rule, then an evaluation is performed on an constraints on the deny rule, if the evaluation finds a presently valid constraint on the deny rule, then access is denied, and if the evaluation finds that all constraints on the deny rule are not presently valid, then a search for a grant rule is performed, and if no deny rules are found, then a search for a grant rule is performed;

wherein after a search for a grant rule if no grant rule is found that would allow access for the user, then access is denied, and if a grant rule is found, then an evaluation is performed on any constraints in the grant rule wherein if the evaluated constraint is presently valid, then access is allowed, and if the evaluated constraint is not presently valid, then access is denied; and, and audit records the authorization request in an audit log;

wherein if there is an error in the authorization request, or if the request is not valid, then access is denied; if the authorization request is valid, then a determination is made whether access should be granted, and if the evaluated authorization request does not deny access, then access is allowed, and if the evaluated authorization request denies access, then access is denied.

157. (Amended) A system for maintaining security in a distributed computing environment, comprising:

a policy manager <u>located at a server</u> for managing a security policy; and

an application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, for managing access to securable components as specified by the security policy, said securable components being selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

167. (Amended) A method for maintaining security in a distributed computing environment, comprising the steps of:

managing a policy using a policy manager located at a server by specifying access privileges of a user to securable components selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application; and

distributing the policy to a client having an application guard, said application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, whereby the application guard manages access to the securable components as specified by the policy,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

169. (Amended) A computer-readable medium comprising program instructions for maintaining security in a distributed computing environment by performing the steps of:

managing a policy using a policy manager located at a server by specifying access privileges of a user to securable components selected from the group consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application; and

distributing the policy to a client having an application guard, said application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, whereby the application guard manages access to the securable components as specified by the policy,

executing said policy manager with a processor to manage and distribute the policy,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

170. (Amended) A system for maintaining security in a distributed computing environment, comprising the steps of:

means for managing a policy using a policy manager located at a server by specifying access privileges of a user to securable components selected from the group

consisting of at least one application, a function within an application, a procedure within an application, a data structure within an application, a database object referenced by an application, or a file system object referenced by an application; and

means for distributing the policy to a client having an application guard, said application guard located either at a client or at a server, said application guard associated with the client or with a set of clients and including a customized local policy particular to said client or set of clients, whereby the application guard manages access to the securable components as specified by the policy,

means for executing the policy manager to manage and distribute the policy,

wherein said system is scalable by further comprising a plurality of clients, including a local security policy for each of said plurality of clients, and an additional application guard associated with each or a set of said plurality of clients, for managing access to the securable components as specified by the local security policy for each client.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BH

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100